TEWKESBURY BOROUGH COUNCIL

Report to:	Executive Committee
Date of Meeting:	29 August 2018
Subject:	Data Protection Policy
Report of:	Head of Corporate Services
Corporate Lead:	Chief Executive
Lead Member:	Lead Member for Corporate Governance
Number of Appendices:	2

Executive Summary:

Tewkesbury Borough Council is fully committed to compliance with the requirements of the Data Protection Act 2018 and General Data Protection Regulations 2016 (GDPR). The Council's Data Protection Policy attached at Appendix 1 describes the Council's arrangements for compliance. The policy was considered at Audit Committee on 18 July 2018 where is was recommended to Executive Committee for approval.

Recommendation:

To APPROVE the Data Protection Policy.

Reasons for Recommendation:

The Council is required to process personal data lawfully in compliance with the requirements of the Data Protection legislation as set out in this report. The policy outlines the Council's legal requirements for processing data and how the Council will meet them.

Resource Implications:

None arising directly from this report.

Legal Implications:

None directly arising from this report.

Risk Management Implications:

The Council recognises that there are risks associated with users processing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks;

- Accidental or deliberate breach of data protection.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office (ICO) as a result of the loss or misuse of data.
- Council reputational damage as a result of a data protection breach.

Performance Management Follow-up:

The Council's Data Protection Officer will monitor this policy on an annual basis. The Council's Senior Information Risk Owner (SIRO) will regularly review the policy, for example, by using Internal Audit to determine if the policy is being adhered to.

Environmental Implications:

None.

1.0 INTRODUCTION/BACKGROUND

1.1 The document attached at Appendix 1 sets the Council's policy for compliance with the Data Protection Act 2018 (DPA) and General Data Protection Regulation 2016 (GDPR) which came into effect on 25 May 2018. The Council must comply with all relevant legislation and maintain good practices to protect the personal data held. This policy also aims to outline the members of the public's rights in gaining access to their personal data held by the Council, and to assist the Information Commissioner's Office (ICO). Those who process data must comply with the statutory requirements which applies to all personal data, and the policy provides guidance to ensure that all personal data is lawfully processed by the Council. The Audit Committee considered the draft policy on 18 July 2018 and have recommended it to the Executive Committee for approval.

2.0 THE PRINCIPLES OF DATA PROTECTION

2.1 Anyone processing personal data must comply with six principles of good practice. Summarised, the principles require that personal data should be:

- Processed lawfully, fairly and in a transparent manner.
- Only obtained for specified, explicit and legitimate purposes.
- Adequate, relevant and not excessive.
- Accurate and kept up to date.
- Not be kept for longer than is necessary.
- Processed in a secure manner.

The principles are detailed within the Data Protection Policy at Appendix 1.

2.2 The Council will ensure that it is able to demonstrate compliance with all of the above six principles by:

- Following best practice in all personal data processing.
- Ensuring the fair and lawful processing of personal data.
- Telling people why we are processing their personal data and who we will share their personal data with, through our clear and effective privacy notices.
- Ensuring that if relying on consent from the data subject, it is freely given, specific, informed and unambiguous.
- Implementing 'privacy by default' measures to ensure that, by default, we only process the personal data necessary for each business purpose.

3.0 ROLES AND RESPONSIBILITIES

3.1 The Council is accountable for and must be able to demonstrate compliance with Data Protection legislation and adherence to the proposed policy. An overview of the roles and responsibilities established to oversee compliance are as follows:

- Senior Information Risk Owner (SIRO) – to ensure that information assets are appropriately managed. Oversees and is responsible for the whole information governance framework and the risk associated with it.
- Data Protection Officer (DPO) – to undertake the statutory role by monitoring compliance and by providing training, advice and assistance to the SIRO.
- Business Administration Manager – acts as the single point of contact for customers, staff, members and the DPO in relation to personal data. Oversees delivery of the GDPR action, providing advice and support to information asset owners.
- Information asset owners (IAO) – each operational manager has been designated as the IAO for their service. It is their responsibility to ensure their services are compliant with data protection legislation.

A summary of the key roles of the SIRO, the Data Protection Officer and the Information Commissioner is set out in Appendix 2. An internal Information Board has been set up to ensure the ongoing compliance with GDPR. The board meets on a monthly basis and is chaired by the SIRO.

4.0 OTHER OPTIONS CONSIDERED

41 None.

5.0 CONSULTATION

5.1 Information board.

Audit Committee 18 July 2018.

6.0 RELEVANT COUNCIL POLICIES/STRATEGIES

6.1 Information Security Policy.

Supports delivery of relevant Council Plan actions.

7.0 RELEVANT GOVERNMENT POLICIES

7.1 Government Security Classifications.

8.0 RESOURCE IMPLICATIONS (Human/Property)

8.1 None.

9.0 SUSTAINABILITY IMPLICATIONS (Social/Community Safety/Cultural/ Economic/ Environment)

9.1 None.

10.0 IMPACT UPON (Value For Money/Equalities/E-Government/Human Rights/Health And Safety)

10.1 As set out in the report

11.0 RELATED DECISIONS AND ANY OTHER RELEVANT FACTS

11 .1 None.

Background Papers: None

Contact Officer: Head of Corporate Services
01684 272002 Graeme.simpson@tewkesbury.gov.uk

Appendices: Appendix 1 – Data Protection Policy
Appendix 2 – Key roles and responsibilities